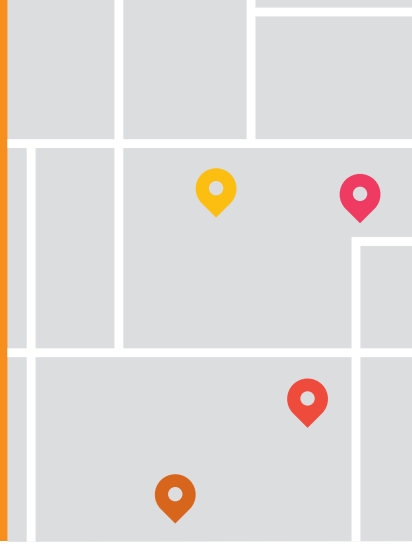
Cyberangriffe früher erkennen und schneller abwenden – mit PwC's Managed Cyber Defence (MCD)



Managed Cyber Defence (kurz MCD) ist eine Kombination der Cortex XDR Lösung von Palo Alto Networks und PwC's Security Operation Center (SOC) Services.

Bekannte Herausforderung

Einbrecher sind leise, agieren im Verborgenen und schlagen schnell zu, um noch schneller mit der Beute zu verschwinden – genau wie Cyberkriminelle. Präventive Sicherheitsmaßnahmen (Firewall, Proxy, etc.) helfen zwar dabei, den Aufwand für den Angreifer zu erhöhen – können jedoch nicht jeden davon abhalten in Unternehmen einzudringen. Präventive Maßnahmen zur Absicherung von Endgeräten reichen oftmals nicht mehr aus. Die klassische Endgerätesicherheit mit ihrem Signatur-basierten Ansatz kann zwar Angriffe erkennen und die Angriffsfläche eines jeden Unternehmens reduzieren – doch sie kann nicht neuartige Attacken abwehren. Möchte man eine umfängliche Cybersicherheit umsetzen, so muss man neben präventiven Maßnahmen auch die Perspektiven „Detektion" von und „Reaktion" auf Sicherheitsvorfälle berücksichtigen. Wer Angriffe schnell erkennt und noch schneller darauf reagieren kann, der kann auch den Schaden und das Ausmaß rechtzeitig minimieren.

Wie wir Ihnen helfen können

Unser Managed Cyber Defence Service ist ein 24/7 Managed Security Service für Palo Alto Networks Cortex XDR Lösung. Endpoint Detection and Response-Lösungen fokussieren sich auf die Detektion von böswilligen Aktivitäten auf Endgeräten (z. B Laptops) und Servern im lokalen Netz. XDR erweitert die Detektion um weiteren Daten aus der Cloud und dem Unternehmensnetzwerk. Dadurch bringt es zusätzliche Aspekte zusammen und liefert ein weitaus vollständigeres Bild eines Angriffs. Unsere SOC-Experten können so Bedrohungen frühzeitig erkennen und mittels unserer XSOAR-Plattform sowie unseres hauseigenen PwC Playbooks (genannt "TERRanCE") unmittelbar auf Angriffe reagieren. Dabei setzen wir zusätzlich auf Best Practices (z. B. Mitre Attack) sowie unsere eigene Threat Intelligence, damit wir immer die neuesten Informationen zu Techniken, Taktiken und Vorgehen von Angreifern vorliegen haben.

Ihre Vorteile

- Schnelle Erkennung und Eindämmung von Sicherheitsvorfällen
- Reduktion von Arbeitsaufwand durch automatisiertes Playbook
- Kosten einsparen im Vergleich zur unternehmensinternen 24/7 Überwachung

Unsere Leistungen im Detail:

Palo Alto Networks Cortex XDR

- Endpoint Protection
- Regelbasierte Analysen
- Verhaltensbasierte Analysen
- Gerätekontrolle
- Investigation- und Response- Funktionen

PwC SOC Service für Cortex XDR

- Implementierung von Cortex XDR
- 24/7 Alarm-Triage durch SOC-Analysten
- PwC Threat Intelligence
- Threat Hunting
- Automatisierung und Orchestrierung mittels XSOAR-Plattform und "TERRanCE" Playbook
- Fortlaufende Weiterentwicklung des Playbooks und von Use Casen
- Zugriff auf das PwC Threat Management Portal

pwc

Warum wir ein starker Partner sind:

Wir kennen Ihre Herausforderungen:

Zu viele Alarme/Meldungen:
EDR-Lösungen bringen zusätzliche Transparenz. Dies bedeutet aber auch eine erhöhte Menge an Daten die analysiert und meist manuell bewertet werden müssen.

Mangel an qualifizierten Fachkräften:
Qualifizierte Security-Fachkräfte sind rar und teuer. Die Weiterbildung von Mitarbeitern ist aufwendig.

Zu wenig Erfahrung bei der Reaktion auf Sicherheitsvorfälle:
Incident Response Pläne sind nicht vorhanden bzw. unzureichend erprobt.

Unsere Managed Cyber Defence Service gemeinsam mit Cortex XDR von Palo Alto Networks ist eine ganzheitliche Lösung: XDR-Lösungen sind zwar technisch sehr fortgeschritten – jedoch benötigt es ein ausgewogenes Verhältnis zwischen qualifizierten Mitarbeitern, erprobten Prozessen und fortgeschrittenen Technologien, um gezielt Angriffe zu vereiteln und auf Incidents reagieren zu können. Daher ergänzt unser Security Operation Center (SOC) Service Palo Alto Networks XDR-Lösung Lösung optimal durch kontinuierliches Security Monitoring (24/7) und tiefgehende Threat-Untersuchung durch SOC-Analysten.

Managed Cyber Defence in Zahlen

Erkannte Angriffe
> 2.000 +

Durchschnittliche Anzahl der täglich bearbeiteten Vorfälle
> 14 Mrd.

9 Fälle
Durchschnittliche tägliche Fallzahl pro Kunde

50 %
Reduzierung des SOC-Personalbedarfs für die L1/L2-Analyse

3
Anzahl der ATP-Gruppen, die durch die Incident Response von MCD entfernt wurden (Q1/2 2020)

Vereinbaren Sie mit unserem Experten ein Erstgespräch:

Achim Schäfer
Partner, Cyber Security & Privacy
PwC Deutschland
Tel.: +49 69 9585-1022

© März 2021 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.

www.pwc.de